ALGEMEEN BELEID BESCHERMING PERSOONSGEGEVENS

RIJKSUNIVERSITEIT GRONINGEN

Inhoud

1. Uitgangspunten

1.1. Inleiding

Door toenemende digitalisering en door toenemende bewustwording van het belang van de bescherming van de persoonlijke levenssfeer van een individu, is privacy een steeds relevanter onderwerp geworden. Eén uitvloeisel van het recht op privacy is de plicht tot een behoorlijke en zorgvuldige omgang met persoonsgegevens. Het College van Bestuur (hierna: CvB) wil dat dit tot in de haarvaten van de Rijksuniversiteit Groningen wordt toegepast. Daartoe heeft het CvB onderhavig beleid (hierna: Privacybeleid) vastgesteld dat in hoofdlijnen de visie en uitgangspunten van de Rijksuniversiteit Groningen ten aanzien van de bescherming van persoonsgegevens beschrijft.

N.b. paragraaf 4 van dit beleid bevat een lijst met definities van de gebruikte begrippen.

1.2. Privacy-visie Rijksuniversiteit Groningen

De RUG heeft als missie het creëren en delen van kennis door middel van excellent onderzoek en onderwijs. De RUG wil zo een substantiële bijdrage aan de samenleving leveren. De privacy-visie van de RUG sluit hierop aan.

Elke student, elke medewerker, elk onderzoekssubject en ieder ander moet erop kunnen vertrouwen dat zijn of haar persoonsgegevens door de RUG rechtmatig worden verwerkt en passend worden beschermd. Te allen tijde gaat de RUG zorgvuldig en behoorlijk om met de persoonsgegevens die de universiteit verwerkt. Door minimaal te voldoen aan de geldende privacywet- en regelgeving biedt de RUG een consistent en hoog niveau van bescherming van de rechten en vrijheden van individuen ('privacyvolwassenheid').

De RUG is daarom transparant over wat zij met persoonsgegevens doet en neemt verantwoordelijkheid, ook als er fouten worden gemaakt. De RUG stelt individuen in staat hun gegevens in te zien en te corrigeren. Hun vragen en eventuele klachten worden serieus genomen en op een correcte manier afgehandeld.

Binnen dit kader wordt excelleren in onderwijs en onderzoek zoveel mogelijk gefaciliteerd en gerealiseerd. Privacyvolwassenheid betaalt zich uit in een positieve bijdrage aan de missie van de RUG.

1.3. Doel

Doel van dit privacybeleid is:

- Het waarborgen van een zorgvuldige, behoorlijke en veilige omgang met de persoonsgegevens die de RUG verwerkt, in overeenstemming met de geldende privacywet- en regelgeving, op een zodanige manier dat de rechten en vrijheden van individuen worden geëerbiedigd;
- Het scheppen van de kaders waarbinnen dit beleid uitgevoerd wordt;
- Het voorkomen van privacy-incidenten en, als deze zich toch voordoen, het beperken van schade voor individuen en de organisatie;

- Het implementeren van maatregelen en mechanismen die de privacyvolwassenheid van de RUG optimaliseren;
- Het faciliteren en activeren van alle medewerkers van de RUG om bij te dragen aan de privacyvolwassenheid van de organisatie;
- Het in staat stellen van het CvB om met vertrouwen verantwoording af te leggen aan betrokkenen en autoriteiten.

1.4. Doelgroep

De doelgroep van dit beleid wordt gevormd door alle medewerkers en studenten van de RUG. De verantwoordelijkheden, taken en bevoegdheden die medewerkers en studenten hebben met betrekking tot de bescherming van persoonsgegevens, zijn nader uitgewerkt in dit privacybeleid en de daaronder hangende richtlijnen, reglementen en gedragscodes. Het beleid wordt ten behoeve van de transparantie over verwerking van persoonsgegevens gedeeld op de publieke website van de RUG.

1.5. Toepassingsbereik

Dit privacybeleid is van toepassing op de verwerking van persoonsgegevens. Persoonsgegevens zijn alle gegevens die betrekking hebben op een natuurlijk persoon en die deze persoon direct of indirect identificeren. Verwerking betreft iedere handeling met betrekking tot persoonsgegevens, zoals inzien, delen, wijzigen, kopiëren, opslaan en vernietigen. Het beleid ziet op de gehele levenscyclus van persoonsgegevens. Het beleid geldt ten aanzien van zowel geautomatiseerde als niet geautomatiseerde verwerking.

Het beleid is van toepassing op de volledige universiteit en al haar faculteiten, diensten en afdelingen. Het is gericht op alle processen binnen de universiteit waarbij persoonsgegevens worden verwerkt, zowel in het kader van onderwijs en onderzoek als in het kader van het faciliteren en ondersteunen van deze primaire taken. Ook wanneer de verwerking van persoonsgegevens wordt verricht door een derde in opdracht van de RUG, gezamenlijk met de RUG of anderszins door of vanwege de universiteit, is dit beleid van toepassing.

1.6. Raakvlakken met en verhouding tot andere beleidsthema's en beleidsstukken

Dit privacybeleid heeft raakvlakken met andere beleidsterreinen binnen de RUG. Dit privacybeleid is zoveel mogelijk in lijn gebracht met het voor die terreinen opgestelde beleid. Het is echter mogelijk dat daarin andere accenten worden gelegd ten aanzien van de bescherming van persoonsgegevens. Deze moeten altijd in het licht van dit privacybeleid beoordeeld worden.

1.7. Juridisch kader

Het juridisch kader voor dit privacybeleid wordt hoofdzakelijk gevormd door de Algemene Verordening Gegevensbescherming (AVG). Daarnaast bestaat nationale uitvoeringswetgeving (bijv. de Nederlandse Uitvoeringswet AVG) en wetgeving die regels stelt voor specifieke vormen van verwerkingen van persoonsgegevens. Verder bestaat wetgeving die specifieke instructies ten aanzien van verwerking geeft, zoals bewaarplichten (bijv. artikel 52 AWR) of

anonimiseringsplichten (bijv. artikel 10 lid 1 sub d Wob). Natuurlijk is in voorkomende gevallen overige wetgeving waaraan de RUG zich dient te houden (bijv. de Wet op het Hoger onderwijs en onderzoek of de Algemene wet bestuursrecht) onderdeel van het juridisch kader. Het voert echter te ver om de verhouding tussen de verschillende wetgeving nader te bepalen in dit beleid. Dit zal bij toepassing van geval tot geval beoordeeld worden.

Naast de toepasselijke wetgeving wordt het juridisch kader bepaald door beleidsregels, gedragscodes en certificeringsmechanismen die door een bevoegde overheidsinstantie (bijvoorbeeld de Autoriteit Persoonsgegevens) zijn vastgesteld. Dit geldt eveneens voor zienswijzen van de Functionaris voor de Gegevensbescherming (hierna: FG). Ook kunnen gedragscodes worden opgesteld vanuit koepels als de VSNU (bijv. gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek) of door de RUG zelf, waaraan de universiteit zich committeert.

1.8. Ingangsdatum en onderhoud

De eerste versie van dit privacybeleid is vastgesteld op 4 juni 2018 door het CvB en is vanaf dat moment van toepassing. Het beleid zal van tijd tot tijd worden aangevuld en gewijzigd. Wijzigingen zijn van kracht na goedkeuring door het CvB. De wijzigingen in deze versie hebben met name betrekking op de inrichting van de privacymanagementorganisatie. De werkplannencyclus is enigszins aangepast en de rollen van Chief Privacy Officer en IT-auditor zijn ingebed in de privacymanagementorganisatie.

2. Privacymanagement

2.1. Managementstructuur

Privacyvolwassenheid van de RUG kan uitsluitend worden gerealiseerd door de inzet van alle bestuurslagen en medewerkers van de universiteit. Daarom heeft dit beleid bewust een activerend karakter en geldt binnen de RUG een structuur die privacymanagement mogelijk maakt. Deze structuur is vastgesteld op basis van een "RASCI Responsibility Matrix" en ziet er als volgt uit:

	Soort verantwoordelijkheid	**Functie**
Responsible	Feitelijke verantwoordelijkheid	Faculteitsbestuur en directie dienst
Accountable (approving)	Eindverantwoordelijkheid	CvB
Supporting	Uitvoerende verantwoordelijkheid	Privacy & security-coördinatoren, onderzoekers, medewerkers en studenten van de RUG
Consulting	Adviserende verantwoordelijkheid	CPO, ABJZ, CISO
		FG, IT-auditor
		Strategische commissie voor privacybescherming en informatiebeveiliging
Informed	Geïnformeerde verantwoordelijkheid	Medezeggenschapsorganen, betrokkenen, externe toezichthouders[1]

Een nadere uitwerking van deze verantwoordelijkheden in omvang, taken en bevoegdheden wordt in het vervolg van dit beleid gegeven. Altijd geldt dat het bestuur of de directie waaronder een persoon met één of meerdere hierboven beschreven functies ressorteert, deze persoon de middelen en tijd geeft om de functie naar behoren uit te voeren.

2.2. Verantwoordelijkheden en bevoegdheden faculteitsbestuur / directies diensten

Besturen van faculteiten en de directies van de diensten van de RUG zijn ervoor verantwoordelijk dat hun faculteit of dienst voldoet aan de privacywetgeving en dit privacybeleid. Het bestuur of de directie draagt de volgende de taken en verantwoordelijkheden:

[1] In paragraaf 3.11 van dit beleid wordt beschreven hoe de RUG verantwoording aflegt aan betrokkenen en toezichthouders.

- Zorgdragen voor bewustwording van het belang van privacyvolwassenheid voor diens faculteit of dienst;
- Het in kaart brengen van alle verwerkingen van persoonsgegevens binnen diens faculteit of dienst, het registreren van deze verwerkingen in het daarvoor bestemde register en het actueel houden van deze registraties;
- Het in kaart brengen van de risico's voor de bescherming van persoonsgegevens die spelen bij de verwerkingen van de organisatie-eenheid en het waarderen en mitigeren van deze risico's;
- Zorgdragen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met de privacywet- en regelgeving;
- Zorgdragen dat een DPIA wordt uitgevoerd en/of de FG tijdig wordt geconsulteerd wanneer dat nodig is op grond van de privacywet- en regelgeving en/of RUG-beleid;
- Het, op basis van een risicoanalyse, realiseren van passende waarborgen voor de bescherming van persoonsgegevens;
- Het monitoren van de privacyvolwassenheid van diens faculteit of dienst;
- Het tijdig en volledig melden van (vermoedelijke) datalekken en privacy-incidenten binnen de faculteit of dienst;
- Het afstemmen met andere faculteiten en diensten over de toepassing van dit beleid, zodat dubbel werk voorkomen wordt.

Het bestuur of de directie stelt jaarlijks een plan van aanpak op waarin bovenstaande verantwoordelijkheden voor de domeinen onderwijs, bedrijfsvoering en wetenschappelijk onderzoek worden uitgewerkt in concrete maatregelen en acties. Dit plan van aanpak is onderdeel van het werkplan voor bescherming van persoonsgegevens en informatiebeveiliging dat faculteiten en diensten jaarlijks op moeten stellen op grond van de universitaire richtlijn voor het maken van het werkplan voor informatiebeveiliging en gegevensbescherming.

Het bestuur van een faculteit is verantwoordelijk voor specifiek de bescherming van persoonsgegevens in het kader van wetenschappelijk onderzoek worden verwerkt. Het faculteitsbestuur ondersteunt de onderzoeker bij het uitvoeren van diens verantwoordelijkheden.

Privacy is een zelfstandig aandachtsgebied van een faculteitsbestuur of directie. Indien een faculteitsbestuur of een directie uit meerdere personen bestaat, wordt besloten wie portefeuillehouder privacy is.

Het bestuur of de directie stelt minimaal één privacy & security-coördinator aan om de toepassing van de privacywet- en regelgeving en dit privacybeleid binnen diens faculteit of dienst te coördineren. Waar dat noodzakelijk is, stelt een faculteitsbestuur of directie van een dienst meerdere privacy & security-coördinatoren aan, bijvoorbeeld voor bepaalde afdelingen. Een faculteitsbestuur of directie kan ervoor kiezen om een privacy-commissie voor haar faculteit of dienst in het leven te roepen. Hierin hebben de portefeuillehouder privacy binnen het bestuur of de directie en de privacy & security-coördinatoren zitting.

De faculteitsbesturen en directies leggen verantwoording af aan het CvB. Zij zorgen ervoor dat telkens in hun jaarlijkse werkplan gerapporteerd wordt over de realisatie van de

voorgenomen acties en maatregelen in het jaar voorafgaand aan het jaar waar het werkplan op ziet. ABJZ ontvangt een afschrift van deze rapportage, die namens het CvB wordt beoordeeld door de Chief Privacy Officer (hierna: CPO), de Chief Information Security Officer (hierna: CISO), de FG en de IT-auditor.

2.3. Verantwoordelijkheden en bevoegdheden College van Bestuur

Het CvB is eindverantwoordelijk voor het beheer van de universitaire gegevensbestanden en de privacyvolwassenheid van de Rijksuniversiteit Groningen. Het CvB is in dat kader voor de externe toezichthouder, de betrokkene en derden aanspreekpunt en legt zo naar buiten toe verantwoording af. Ook informeert het CvB de universiteitsraad en de Raad van Toezicht waar nodig over de ontwikkelingen op dit vlak. Het CvB kan zich bij het afleggen van verantwoording en het geven van informatie laten ondersteunen door de FG. Het CvB stelt beleid vast dat bepaalt hoe de FG tijdig en in voldoende mate wordt betrokken bij aangelegenheden die de bescherming van persoonsgegevens betreffen.

Het CvB stelt jaarlijks, op basis van de jaarrapportage van de FG, vast hoe de RUG groeit in privacyvolwassenheid. Dit gebeurt door middel van een managementreactie op de rapportage. De managementreactie wordt door de CPO voorbereid. Het CvB faciliteert de gremia en medewerkers van de RUG in het voldoen aan de privacywet- en regelgeving en stelt hiervoor middelen en ondersteuning beschikbaar. Wanneer een faculteitsbestuur of directie van een dienst in gebreke is met betrekking tot de privacywet- en regelgeving of dit privacybeleid, treft het CvB in redelijkheid de maatregelen of sancties om dit te herstellen.

2.4. Verantwoordelijkheden en bevoegdheden privacy & security-coördinatoren, procesbeheerders en medewerkers

2.4.1. Algemeen

Privacy & security-coördinatoren, procesbeheerders, onderzoekers en medewerkers werken onder verantwoordelijkheid van het faculteitsbestuur of directie van de dienst waar zij onder ressorteren.

2.4.2. Verantwoordelijkheden en bevoegdheden privacy & security-coördinatoren

Elke faculteit of dienst binnen de RUG heeft minimaal één privacy & security-coördinator die ondersteunt bij het privacyvolwassen maken van diens faculteit of dienst en de uitvoering van de taken van diens bestuur of directie coördineert. De privacy & security-coördinator is het eerste aanspreekpunt voor privacygerelateerde vragen van de medewerkers van diens faculteit of dienst. Tevens brengt de coördinator de verwerkingen van persoonsgegevens in kaart en registreert hij ze in het daarvoor bestemde register. De privacy & security-coördinator legt verantwoording af aan diens bestuur dan wel directie.

2.4.3. Verantwoordelijkheden en bevoegdheden medewerkers

Alle medewerkers van de Rijksuniversiteit Groningen gaan zorgvuldig om met de persoonsgegevens die zij verwerken. Ze nemen kennis van de hiervoor opgestelde

beleidsstukken, richtlijnen en instructies en leven die na. Zij ondersteunen waar nodig en mogelijk de organisatie met hun kennis en kunde. Wanneer zij kennisnemen van mogelijke privacy-incidenten, rapporteren zij deze zo snel mogelijk bij de daarvoor ingerichte meldpunten of de FG.

2.4.4. Verantwoordelijkheden en bevoegdheden van onderzoekers

De onderzoeker heeft een zelfstandige verantwoordelijkheid voor de privacyvolwassenheid van diens onderzoek. Bij de invulling van deze verantwoordelijkheid is een rol weggelegd voor de ethische commissies. Zijn zien, namens het faculteitsbestuur, toe op de toetsing van het onderzoek aan ethische en juridische eisen. De onderzoeker conformeert zich aan de privacywet- en regelgeving, gedragscodes in het veld en facultair beleid. Ondersteuning vindt, naast de reguliere ondersteuning binnen de faculteit, plaats door het Groningen Data Competence Center (hierna: GDCC).

2.4.5. Verantwoordelijkheden en bevoegdheden van studenten

Studenten van de RUG kunnen in het kader van hun opleiding toegang krijgen tot persoonsgegevens. Studenten gaan zorgvuldig met de persoonsgegevens om en conformeren zich aan universitair beleid en de instructies die zij ontvangen van hun docenten en begeleiders. Faculteiten zijn verantwoordelijk voor het begeleiden van studenten bij het gebruik van persoonsgegevens in onderzoek.

2.5. Verantwoordelijkheden en bevoegdheden CPO, ABJZ en CISO

2.5.1. Verantwoordelijkheden en bevoegdheden CPO

De Chief Privacy Officer (CPO) is verantwoordelijk voor het ontwikkelen en implementeren van het universitaire privacybeleid, met inbegrip van richtlijnen en procedures voor het beschermen van persoonsgegevens van studenten, personeel, onderzoeksubjecten en andere individuen. De CPO bewaakt dat de faculteit en diensten handelen volgens dit beleid en dat de daaruit vloeiende maatregelen toegepast worden. De CPO geeft faculteiten en diensten advies bij het opstellen en uitvoeren van het werkplan en geeft de privacy- & securitycoördinatoren inhoudelijke ondersteuning. De CPO adviseert het CvB over de opvolging van de jaarrapportage en de adviezen van de FG.

De CPO adviseert over complexe privacy-aangelegenheden, initieert risico-analyses en privacy-audits, organiseert awarenessprogramma's, en adviseert bestuur en management. De CPO zorgt voor overzicht van en sturing op de privacyrisico's die spelen binnen de universiteit. De CPO rapporteert over diens werkzaamheden aan de Strategische commissie voor privacybescherming en informatiebeveiliging en is werkzaam bij de afdeling ABJZ.

2.5.2. Verantwoordelijkheden en bevoegdheden ABJZ

ABJZ adviseert faculteiten en diensten bij de toepassing van de privacywet- en regelgeving binnen de RUG. ABJZ begeleidt DPIA's, stelt verwerkersovereenkomsten op en werkt privacyverklaringen uit. ABJZ ondersteunt alle medewerkers en in het bijzonder de privacy & security-coördinatoren, procesbeheerders, onderzoekers en de FG bij het uitvoeren van hun taken. ABJZ adviseert onderzoekers bij samenwerking over compliance, uitzonderingen voor

onderzoek en voorwaarden van onderzoeksfinanciers. ABJZ adviseert bij nadere uitwerking van dit privacybeleid. ABJZ stemt haar werkzaamheden voortdurend af met de FG, CPO en de CISO.

2.5.3. Verantwoordelijkheden en bevoegdheden CISO

De Chief Information Security Officer (CISO) is verantwoordelijk voor het ontwikkelen en implementeren van het universitaire informatiebeveiligingsbeleid, met inbegrip van richtlijnen en procedures voor het beschermen van de universitaire informatiesystemen tegen interne en externe dreigingen. De CISO is verantwoordelijk voor het functioneren van het Information Security Management Systeem en bewaakt dat de universiteit voldoet aan het informatiebeveiligingsbeleid. De CISO rapporteert hierover aan de Strategische commissie voor privacybescherming en informatiebeveiliging. De CISO is werkzaam bij het CIT.

De CISO ondersteunt de RUG bij het treffen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen ongeoorloofde toegang en onrechtmatige verwerking. De CISO is voorzitter van het Computer Emergency Response Team (CERT) van de RUG.

2.6. Verantwoordelijkheden en bevoegdheden FG en IT-auditor

2.6.1. Verantwoordelijkheden en bevoegdheden FG

De FG is verantwoordelijk voor het geven van gevraagd en ongevraagd advies over en het toezicht houden op de naleving van de privacywet- en regelgeving en het privacybeleid. De FG heeft binnen de RUG minimaal de taken, verantwoordelijkheden en bevoegdheden die hem op grond van de privacywet- en regelgeving worden toegekend.

De FG heeft toegang tot iedere informatie van de RUG die betrekking heeft op verwerking van persoonsgegevens – zowel tot de persoonsgegevens zelf als tot de verwerkingsactiviteiten en de systemen waarmee die activiteiten worden verricht. Het CvB kan bepalen dat, voor toegang tot bepaalde informatie wordt verkregen, voorafgaand melding wordt gedaan aan het CvB. De FG houdt toezicht op het register voor de verwerkingsactiviteiten.

De FG wordt in staat gesteld taken uit te voeren en zijn deskundigheid in stand te houden. De FG rapporteert direct aan het CvB. De FG brengt jaarlijks een rapportage uit over de bescherming van persoonsgegevens binnen de RUG. De rapportage wordt beschikbaar gesteld aan het CvB en de Raad van Toezicht. De rapportage wordt ter informatie toegezonden aan de universiteitsraad.

De FG ondersteunt het CvB in het afleggen van verantwoording naar buiten toe, zowel aan toezichthouders als aan betrokkenen. De FG onderhoudt daarvoor contact met de toezichthoudende autoriteiten. De FG geeft aanbevelingen die strekken tot verdere optimalisering van de privacybeleidsvoering.

2.6.2. Verantwoordelijkheden en bevoegdheden IT-auditor

De interne IT-auditor monitort het risicomanagement en de effectiviteit van de risicomitigerende maatregelen ten aanzien van de universitaire processen en informatiesystemen. De IT-auditor van de RUG toetst in opdracht van het CvB en de FG de opzet, het bestaan en de werking van het universitaire privacybeleid en maatregelen die risico's voor de bescherming van persoonsgegevens mitigeren. De IT-auditor brengt deze werkzaamheden onder in een universitair auditplan. De IT-auditor brengt van diens werkzaamheden verslag uit aan de Strategische commissie voor privacybescherming en informatiebeveiliging.

2.7. Verantwoordelijkheden en bevoegdheden strategische commissie voor privacybescherming en informatiebeveiliging

De Strategische commissie voor privacybescherming en informatiebeveiliging adviseert het CvB over de ontwikkeling van universiteitsbreed beleid en werkprogramma's op het gebied van privacy en informatiebeveiliging. De commissie bewaakt dat gegevensbescherming en informatiebeveiliging in lijn zijn met de strategische doelen van de universiteit. De commissie adviseert het CvB over de universitaire risicostrategie en de vereisten voor het voldoen aan wet- en regelgeving. De commissie bestaat uit een lid van het CvB (tevens voorzitter), een tweetal leden van het managementberaad, de CISO en de CPO. De IT-auditor en de FG zijn adviserende leden.

2.8. Verantwoordelijkheden en bevoegdheden medezeggenschapsorganen

Voor zover dat vereist is op grond van de wet of intern beleid, worden de medezeggenschapsorganen van de RUG in staat gesteld hun bevoegdheden uit te oefenen ten aanzien van de wijze waarop de RUG uitvoering geeft aan de privacywet- en regelgeving.

3. Toepassing privacybeleid

3.1. Werkprogramma privacyvolwassenheid College van Bestuur en beleidsevaluatie

De RUG hanteert een gangbaar model voor privacyvolwassenheid. Dit is het “Privacy Volwassenheidsmodel” van het Centrum voor Informatiebeveiliging en Privacy. De RUG heeft zich ten doel gesteld te acteren op minimaal een volwassenheidsniveau van gemiddeld 3.0 volgens dit model. Hiermee worden de in hoofdstuk 1 geformuleerde missie, visie en doelen behaald. Bij het toepassen van het model wordt rekening gehouden met de structuur en cultuur van de organisatie. Het College van Bestuur stelt jaarlijks, in reactie op de jaarrapportage van de FG en het beeld van het universitaire volwassenheidsniveau, in een werkprogramma vast wat gedaan moet worden om het gewenste niveau te bereiken en te behouden. Het werkprogramma wordt door de CPO voorbereid. De uitvoering ervan wordt door de CPO ondergebracht in de universitaire *Plan Do Check Act*-cyclus voor gegevensbescherming en de CPO bewaakt dat het werkprogramma wordt ingebed in de werkplannen van faculteiten en diensten.

3.2. PDCA-cyclus, werkplan faculteiten en diensten

Het faculteitsbestuur en de directies van de diensten zijn ervoor verantwoordelijk dat zij een *Plan Do Check Act*-cyclus implementeren waarmee zij het privacyvolwassen maken en houden van de processen binnen hun faculteit of dienst realiseren. In dat kader stellen zij vast hoe en wanneer het bestuur of de directie uitvoering geeft aan de in paragraaf 2.2 beschreven taken en verantwoordelijkheden. Zij doen dat door jaarlijks een werkplan op te stellen en volgen hierbij de universitaire richtlijn voor het maken van het werkplan voor informatiebeveiliging en gegevensbescherming en de instructies van de CISO en CPO. Hierin passen zij hun taken en verantwoordelijkheden toe met concrete acties en maatregelen ten aanzien van processen en systemen, zodat de privacyvolwassenheid van hun faculteit of dienst verder wordt geoptimaliseerd. Dit werkplan wordt toegezonden aan het CvB en namens het CvB beoordeeld door de FG, CPO, IT-auditor en de CISO van de universiteit. Het faculteitsbestuur of de directie ontvangt hiervan een terugkoppeling. Het CvB ontvangt de beoordeling en deze wordt ter bespreking geagendeerd voor het managementberaad. Daarna wordt de beoordeling ter informatie toegezonden naar het College van Decanen. ABJZ coördineert dit proces.

3.3. Privacy by Design & by default, DPIA’s

Innovatieve onderzoeksprojecten en nieuwe processen binnen de RUG, alsmede de systemen die deze processen ondersteunen, zijn zo opgezet dat de privacy-impact zo laag mogelijk is, terwijl de legitieme doeleinden van deze processen gerealiseerd worden. Privacy by design en privacy by default hebben een plek in het proces voor aanschaffen, ontwikkelen en implementeren van informatiesystemen.

Waar dat nodig is, wordt een DPIA uitgevoerd. De RUG heeft een protocol dat bepaalt wanneer dit verplicht is en dat het delen van inzichten uit de DPIA’s stimuleert. Het protocol

sluit minimaal aan bij de eisen van de privacywet- en regelgeving en regelt wanneer een ondersteunende rol van ABJZ vereist is. Faculteitsbesturen en directies zijn verantwoordelijk voor de naleving van dit protocol. Wanneer een DPIA is uitgevoerd, wordt dit geregistreerd in het register als bedoeld in paragraaf 3.5.

3.4. Gedragscodes en certificeringen

De RUG conformeert zich waar mogelijk en redelijk aan gedragscodes en certificeringseisen die een zorgvuldige en behoorlijke omgang met persoonsgegevens bevorderen. Het CvB besluit in het jaarlijkse werkprogramma aan welke gedragscodes de RUG zich conformeert. De FG kan de RUG adviseren zich te conformeren aan gedragscodes.

3.5. Register voor de verwerkingsactiviteiten

Alle verwerkingen van persoonsgegevens door of namens de RUG, worden geregistreerd in een centraal register onder verantwoordelijkheid van ABJZ. Dit register voldoet aan de eisen van de privacywet- en regelgeving, maar is daarnaast een instrument om privacyvolwassenheid te realiseren en daarover verantwoording af te kunnen leggen. ABJZ zorgt, in samenspraak met de CPO en FG, ervoor dat het register hiervoor gebruikt kan worden en stelt de te registreren informatie vast. Het register is geschikt voor alle verwerkingen die de RUG uitvoert, zowel in de hoedanigheid van verantwoordelijke als van verwerker in de zin van de privacywet- en regelgeving.

3.6. Informatiebeveiliging

Het informatiebeveiligingsbeleid van de RUG en de daaronder hangende baseline met maatregelen, voorziet in een passende beveiliging van persoonsgegevens tegen onrechtmatige verwerking en onbevoegde toegang. De maatregelen zijn zowel technisch als organisatorisch van aard. Het informatiebeveiligingsbeleid is van toepassing op iedere verwerking van persoonsgegevens door de RUG, al dan niet met inzet van externe partijen (verwerkers) of gezamenlijk met een andere verantwoordelijke. Persoonsgegevens zijn ten minste geclassificeerd als ‘vertrouwelijk’ in de zin van het informatiebeveiligingsbeleid. Per proces waarbinnen persoonsgegevens worden verwerkt, wordt echter beoordeeld of dit niveau passend is. Faculteitsbesturen en directies van diensten zijn hiervoor verantwoordelijk.

3.7. Privacy-incidenten

(Vermoedelijke) datalekken en andere (beveiligings)incidenten waardoor inbreuk wordt gemaakt op de bescherming van persoonsgegevens kunnen worden gemeld bij een daarvoor ingericht meldpunt bij het CIT. De meldingen worden behandeld volgens het Protocol meldplicht datalekken van de RUG. Het protocol wordt jaarlijks geëvalueerd door de CPO, de CISO en de FG. Gemelde datalekken worden geregistreerd in het in paragraaf 3.5 bedoelde register.

3.8. Verwerking van persoonsgegevens van de RUG door derden

De RUG kan de verwerking van persoonsgegevens uitbesteden aan derden, samen met derden verrichten of de persoonsgegevens aan derden verstrekken. ABJZ ondersteunt bij het

beoordelen van de rechtmatigheid van de verstrekking. Als de verwerking door een derde doorgang vindt, worden met deze partij schriftelijke afspraken gemaakt die ervoor zorgen dat een zorgvuldige en behoorlijke omgang met persoonsgegevens gewaarborgd is. De afspraken voldoen aan de eisen van de privacywet- en regelgeving, waaronder artikel 26 en 28 van de AVG. ABJZ werkt, in samenspraak met de FG, modelovereenkomsten uit die door medewerkers van de RUG kunnen worden gebruikt om voor te leggen aan derden. Het daadwerkelijke afsluiten van de overeenkomsten dient altijd te gebeuren conform de instructies van ABJZ. Ondertekening gebeurt door of namens het CvB. Waar instellingsoverstijgend samengewerkt wordt aan afspraken met betrekking tot de verwerking van persoonsgegevens, vervullen ABJZ en de FG een afstemmende rol. ABJZ zorgt voor een proces waarmee de naleving van verwerkersovereenkomsten wordt gemonitord.

3.9. Internationale gegevensuitwisseling

Het verwerken van persoonsgegevens buiten de Europese Economische Ruimte (EER) is uitsluitend mogelijk indien passende waarborgen zijn getroffen voor de bescherming van de persoonsgegevens volgens de privacywet- en regelgeving. Voorafgaand aan een dergelijke verwerking, zal altijd de FG of ABJZ aanwijzingen geven voor het treffen van deze waarborgen.

3.10. Transparantie en rekenschap

3.10.1. Privacyverklaring

Betrokkenen worden volledig, tijdig en in begrijpelijke taal geïnformeerd over de verwerking van hun persoonsgegevens door de RUG. Er is een RUG-brede privacyverklaring waar de betrokkene op wordt gewezen voorafgaand aan de verwerking van zijn persoonsgegevens.

Betrokkenen dienen voor specifieke verwerkingen ook een specifieke privacyverklaring voorgelegd te krijgen, die de RUG-brede privacyverklaring aanvult en daarnaar verwijst. Het faculteitsbestuur en de directies van de diensten zijn ervoor verantwoordelijk dat deze specifieke privacyverklaring wordt opgesteld en voorgelegd. Zij stemmen dit af met de FG of ABJZ. Dit gebeurt bij wetenschappelijk onderzoek in afstemming met de ethische commissie. Een dergelijke aanvullende privacyverklaring wordt in ieder geval opgesteld wanneer de gegevens worden verwerkt op basis van de toestemming van de betrokkene. Aanvullende privacyverklaringen worden geregistreerd bij ABJZ.

3.10.2. Rechten van de betrokkene

Alle verzoeken, vragen en klachten van een betrokkene met betrekking tot de verwerking van zijn persoonsgegevens door de RUG, worden tijdig, zorgvuldig en behoorlijk beoordeeld en afgehandeld. Hiervoor is een *Centraal Loket Privacy* ingericht bij ABJZ. Er is een protocol voor de afhandeling van de berichten die binnenkomen bij het loket. Hierin wordt beschreven hoe wordt omgegaan met verzoeken van betrokkene op grond van de privacywet- en regelgeving (bijvoorbeeld een inzageverzoek of een verzoek tot verwijdering van diens persoonsgegevens). Een betrokkene wordt in iedere privacyverklaring geïnformeerd over diens rechten en over het Centraal loket privacy.

3.10.3. Verantwoording aan privacytoezichthouders

Het CvB legt verantwoording af aan de bevoegde nationale en internationale privacytoezichthouders en de Raad van Toezicht. Het CvB is verantwoordelijk voor het verstrekken van de volledige informatie en het inzichtelijk maken van de privacyvolwassenheid van de RUG.

3.11. Communicatie en PR

Alle medewerkers worden geïnformeerd over dit privacybeleid en de taken en verantwoordelijkheden die zij op grond daarvan hebben. Hiertoe is een website ingericht op het intranet van de RUG. De website wordt gevuld met informatie over de privacywet- en regelgeving, werkinstructies en contractmodellen. De RUG maakt daarnaast op de publieke website informatie openbaar over de omgang met persoonsgegevens en de privacy-visie van de universiteit. De informatie wordt opgesteld en onderhouden door de afdeling Communicatie van het Bureau van de RUG, in samenwerking met ABJZ.

In het geval van een privacy-incident of andere mogelijke privacy-gerelateerde PR-issues, legt het CvB verantwoording af aan betrokkenen, toezichthouder en andere stakeholders. De FG kan, altijd in overleg met het CvB, verantwoording afleggen namens het CvB.

3.12. Bewustwording en training

De RUG werkt voortdurend aan bewustwording op het gebied van privacyvolwassenheid. Zo worden bijvoorbeeld richtlijnen opgesteld die zorgvuldig omgaan met persoonsgegevens stimuleren. Alle medewerkers van de RUG worden in staat gesteld om een training te volgen waarmee zij op de hoogte worden gebracht op de voor hen relevante onderdelen van de privacywet- en regelgeving.

3.13. Aard van dit privacybeleid

Dit privacybeleid geeft algemene richtlijnen voor het realiseren van privacyvolwassenheid, maar beschrijft niet de voorwaarden die kunnen gelden voor een specifieke verwerkingsactiviteit. Voor iedere verwerkingsactiviteit dient bewust en separaat onderzocht te worden hoe deze in overeenstemming wordt gebracht met wet- en regelgeving en dit beleid.

3.14. Toepassing en nadere uitwerking privacybeleid, richtlijnen

Een bevoegdheid om af te wijken van dit privacybeleid wordt, indien aanwezig, in dit beleid expliciet benoemd.

ABJZ werkt, namens het CvB en in samenwerking met de privacy & security-coördinatoren, universiteitsbrede richtlijnen uit die voorschrijven hoe medewerkers, procesbeheerders of privacy & security-coördinatoren dienen te handelen met betrekking tot de omgang met persoonsgegevens. Een faculteitsbestuur of directie van een dienst kan dit doen voor de faculteit of dienst. ABJZ vraagt zo nodig advies van de CPO, FG en/of de CISO voorafgaand aan de vaststelling van een richtlijn.

4. Definities gebruikte begrippen

De in dit privacybeleid gehanteerde begrippen worden als volgt gedefinieerd:

- ABJZ: de afdeling Algemeen Bestuurlijke en Juridische Zaken van de RUG;
- AVG: de Algemene Verordening Gegevensbescherming;
- Betrokkene: de natuurlijke persoon van wie persoonsgegevens worden verwerkt;
- CISO: de Chief Information Security Officer van de RUG;
- CPO: de Chief Privacy Officer van de RUG;
- CvB: het College van Bestuur van de RUG;
- DPIA: Data Protection Impact Assessment (Nederlands: Gegevensbeschermingseffectbeoordeling), een beoordeling van de privacy-impact van een proces of systeem waarbinnen persoonsgegevens worden verwerkt;
- FG: de Functionaris voor de Gegevensbescherming van de RUG;
- Groningen Data Competence Center (GDCC): een samenwerking van de Universiteitsbibliotheek en het Centrum voor Informatietechnologie van de RUG ter ondersteuning onderzoekers en onderzoeksinstituten bij datamanagement;
- Persoonsgegevens: alle gegevens die betrekking hebben op een natuurlijk persoon en deze persoon direct of indirect identificeren;
- Privacyvolwassenheid: het voldoen aan de privacywet- en regelgeving en het waarborgen van een zorgvuldige en behoorlijke omgang met persoonsgegevens;
- Privacy & security-coördinator: de medewerker van de RUG die door een faculteitsbestuur of directie van een dienst is aangewezen om de privacyvolwassenheid van een faculteit, dienst of een afdeling daarvan te coördineren;
- Privacyverklaring: de verklaring, formulier voor informed consent of een ander document waarin de betrokkene wordt geïnformeerd over de verwerking van diens persoonsgegevens door de RUG;
- Privacywet- en regelgeving: alle nationale of internationale wet- en regelgeving die van toepassing is op de RUG en voorwaarden stelt ten aanzien van het verwerken van persoonsgegevens, waaronder de AVG;
- Procesbeheerder: de medewerker van de RUG die binnen een faculteit of dienst ervoor verantwoordelijk is dat een proces of meerdere bij elkaar horende processen worden uitgevoerd of verantwoordelijk is voor de systemen die deze processen ondersteunen;
- Privacybeleid: onderhavig algemeen beleid bescherming persoonsgegevens van de RUG;
- Privacy-impact: de nadelige gevolgen van een proces of verwerking voor de zorgvuldige en behoorlijke omgang met persoonsgegevens en voor de bescherming van de persoonlijke levenssfeer van een betrokkene;
- RUG: Rijksuniversiteit Groningen;
- Strategische commissie voor privacybescherming en informatiebeveiliging: de strategische commissie die het CvB adviseert over de toepassing van dit privacybeleid in relatie tot de strategische doelen van de RUG.
- Verwerking, verwerken: iedere handeling/ieder handelen met betrekking tot persoonsgegevens, zoals inzien, delen, wijzigen, kopiëren, opslaan en vernietigen;

- Verwerker: iedere (rechts)persoon of organisatie die namens de RUG persoonsgegevens verwerkt.

Laatstelijk gewijzigd op 29 november 2021.